REMARKS/ARGUMENTS

Applicant thanks Examiner for the detailed Office Action of January 17, 2006.

The Office Action has been carefully considered. It is respectfully submitted that the issues raised are traversed, being hereinafter addressed with reference to the relevant headings appearing in the Detailed Action section of the Office Action.

Claim Rejections – 35 USC § 103

At page 3 of the Office Action, the Examiner rejects claims 1 to 6, 8, 9, 11 to 19, 21, 22, and 24 to 27 as being unpatentable over Shigenaga (US Patent No. 4,710,613) in view of Lee (US Patent No. 5,923,759.

Reconsideration and withdrawal of this rejection is respectfully requested in light of the following comments.

Claim 1 specifies the steps of:

*"applying in the untrusted authentication chip, an asymmetric encrypt function to the first decrypted outcome **together with an original data message read from the untrusted authentication chip** using the second secret key to produce a second encrypted outcome"*

and

*"comparing the decrypted random number **and decrypted data message** with the original random number and the received original data message..."*

The Examiner has acknowledged on page 4 of the Office Action that *"Shigenaga does not disclose...an original data message read from the untrusted authentication chip"*. Thus, the Applicant assumes the Examiner must be relying on Lee for showing this particular feature of the above step.

However, it is apparent from the Examiner comments on pages 4 and 5 that Lee has only been relied upon for disclosing an encryptor module and decryptor module both in the terminal and card. The Examiner has not shown that the card *applies an asymmetric encrypt function to the first decrypted outcome **together with an original data message read from the untrusted authentication chip** using the second secret key to produce a second encrypted outcome"*, or that there is a comparison of decrypted data message with the original data message. Furthermore, Lee only discloses encrypting the random number received from the terminal. Lee does not disclose reading and encrypting an original data message read from the untrusted authentication chip as well as the random number. The MPEP states at 2143 "*Basic Requirements of a Prima Facie Case of Obviousness*" that:

> "... *three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.*
>
> *The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure. In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).*"

As the Shigenaga in view of Lee does not disclose the card "*applying an asymmetric encrypt function to the first decrypted outcome* ***together with an original data message read from the untrusted authentication chip*** *using the second secret key to produce a second encrypted outcome*", the references in combination do not teach all the claim limitation and thus the third basic requirement of a prima facie case of obviousness has not been met by the Examiner to reject claim 1. As all three basic requirements of a prima facie case of obviousness must be met in order to reject the claim as obvious and therefore unpatentable, the Applicant respectfully requests that the Examiner withdraw the claim rejection. Similar comments also apply to Claim 14, and therefore the claim rejection should also be withdrawn to this claim.

The Examiner has also stated at the bottom of page 4 that Lee discloses the IC card performing both an encryption and decryption function using an internal key stored in the card and the terminal card performs both encryption and decryption using an identifying key stored in memory (column 6, lines 37-67).

We draw the Examiner's attention that although Lee teaches performing encryption and decryption in the IC card and system 100 work in a very different way to which the claimed method and system work.

Lines 37 to 52 of column 6 of Lee describe an Authenticate Card Routine 300 to determine whether a card inserted in one of the card units of the system is authentic. In this routine, the processor 122 generates a random number (herein referred to as $Random_P$), which is sent to the card to be encrypted and then transferred back to the processor 122 to be decrypted to determine whether the card in authentic.

Now in contrast, a separate routine is described at lines 53 to 67 called Authenticate Host Routine 310 which allows a card to determine whether the processing system in which the card is inserted is authentic. Under this routine 310, the card generates a random number (herein referred to an $Random_C$), which is then transferred to the processor 122 which is encrypted and then transferred back to the card to be decrypted by the card.

Thus, it is apparent that each routine, 300 and 310, operate with two separate random numbers, $Random_P$ and $Random_C$. Furthermore, each routine is performed for very separate purposes, as 300 is performed to authenticate the card, whereas 310 is performed to authenticate the processor. Each of these routines are performed totally independently of each other as each operates on separate random numbers. Therefore, although the Applicant acknowledges that Lee does teach the use of an encyrptor and decryptor in the terminal and IC card, it must also be similarly acknowledged by the Examiner that Lee teaches two separate routines which are independent of one another.

If a person skilled in the art were to modify Shigenaga with Lee, it could be apparent to the skilled person in the art that an encyrptor and decryptor could be included in both the IC terminal and IC card. However, this modification should be in light of what was taught by Lee which is that two separate routines are performed to authenticate the card to the terminal, and the terminal to the card. There is no teaching or suggestion in Lee that routine 300 should be dependent on the result of routine 310.

There is no teaching or suggestion in Lee that the encryptor and decryptor in the terminal should encrypt and decrypt the same random number. Furthermore, there is no teaching or suggestion in Lee that the encryptor and decryptor in the card should encrypt and decrypt the same random

number. Lee actually teaches the very opposite by suggesting that routines 300 and 310 are performed independently of each other by encrypting and decrypting $Random_P$ and $Random_C$.

Although the Examiner has provided some motivation to combine Shigenaga with Lee, Shigenaga needs to be substantially modified to encrypt the output of the decryption module as well as an original data message read from the authentication. The modification has not been supported by the prior art. The MPEP states at §2143 that:

> *The teaching or suggestion to make the claimed combination and the reasonable expectation of success* ***must both be found in the prior art, not in applicant's disclosure****. In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)."*

There is no teaching or suggestion in Shigenaga that the output of a decryption module can be used as the input for an encryption module. Furthermore, there is no teaching or suggestion in Lee that the output of a decryption module can be used as the input for an encryption module. Moreover there is no teaching or suggestion that an original data message can be read from the untrusted chip and encrypted together with the decrypted data. Thus, for the Examiner to make such a modification to Shigenaga in view of Lee without any suggestion from either disclosure of Shigenaga or Lee would appear to be unjustified. This modification would represent inventive ingenuity which should not be used to reject a claim as obvious.

Even if the Examiner states that such a combination and modification is supported by Shigenaga or Lee, the MPEP states at §2143.01 (III) that:

> *The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. In re Mills, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990)*

There is no suggestion in Shigenaga or Lee that there would be any desirability of using the output of the decryption module as the input for the encryption module. Furthermore, there is no suggestion of a desirability to read an original data message from the untrusted chip which is to be encrypted with the decrypted random number. The desirability which the Examiner has provided (*because the IC card 2 can apply the encrypt function using a secret key to encrypt the decryption data before sending to the card terminal 1, the card terminal can apply the decrypt function using the public key to decrypt the encrypted data, thus the communication from the IC card 2 to the card terminal 1 is more secure with the encrypted data*) has no support from the prior art. Furthermore, the desirability provided by the Examiner is absolutely irrelevant toward the feature of the original data message which is encrypted together with the decrypted data. The desirability **must** be taught by the prior art, and the desirability that the Examiner has provided is simply not supported by the prior art.

Furthermore, the MPEP states at §2143.01 (II) that:

> *Where the teachings of two or more prior art references conflict, the examiner must weigh the power of each reference to suggest solutions to one of ordinary skill in the art, considering the degree to which one reference might accurately discredit another. In re Young, 927 F.2d 588, 18 USPQ2d 1089 (Fed. Cir. 1991)*

Lee teaches that the encryption modules in the card and terminal receive the random number in unencrypted form. However, in total contrast, Shigenaga teaches that the random number is received in the card in an encrypted form and that a decryptor is used to decrypt the encrypted random number. The response back to the terminal is not encrypted in Shigenaga.

However, in total contrast Lee teaches the response should be encrypted. Thus Lee teaches receiving an unencrypted random number, whereas in total contrast Shigenaga teaches receiving an encrypted random number. Furthermore, Shigenaga teaches sending a response which is unencrypted, whereas Lee teaches that the response is encrypted. These portions of each disclosure are in total conflict. Thus, the Examiner should weigh the power of each of these references and conclude that each reference is teaching the very opposite of each other. Such opposite teachings would be highly unlikely for a skilled person in the art to consider obvious to combine and modify since they strikingly conflict with each other in their functional operation.

The Applicant has also amended claim 1 and 14 to further clarify that the method and system relate to determining whether the consumable can be consumed by the consuming device. Support for this amendment can be found generally on page 32 of the specification as well as other areas of the specification relating to authenticating whether the consumable can be validly consumed.

The Examiner has stated that although Shigenaga does not disclose the trusted authentication chip is contained within a consuming device, and the untrusted authentication chip is contained within the consumable, Shigenaga is an analogous art.

The MPEP states at § 2141.01(a):

> *"In order to rely on a reference as a basis for rejection of an applicant's invention, the reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the inventor was concerned."* In re Oetiker, 977 F.2d 1443, 1446, 24 USPQ2d 1443, 1445 (Fed. Cir. 1992).

The Applicant submits that Shigenaga is not in the field of the applicant's endeavor, and furthermore, Shigenaga is not reasonably pertinent to the particular problem with which the inventor was concerned.

In regard to the first question (field of applicant's endeavour), the Shigenaga citation involves an Intergrated Circuit card which is identified by an Integrated Circuit Terminal using a specific algorithm relating to encryption and estimated processing times. The Shigenaga citation can hardly be considered by the Examiner as being in the field of the applicant's endeavor when the applicant's method and system relate to authenticating whether a consumable containing an untrusted chip can be consumed by a consuming device containing a trusted chip. There is absolutely no reference to consumables in the Shigenaga citation and surely this must indicate to the Examiner that the Shigenaga citation cannot be considered to be in the field of applicant's endeavor. Thus, the Applicant respectfully submits that the answer to the first question should be answered in the negative by the Examiner.

In regard to the second question (reasonably pertinent to the particular problem with which the inventor was concerned), the problem which the applicant is attempting to solve is to ensure that a consumable which was not validly manufactured for the consuming device would not be consumed by the consuming device, and that only a valid consumable would be consumed by the consuming device. If a non-valid consumable is used with the consuming device, problems associated with the consumable malfunctioning can lead to the consuming device also malfunctioning. This can also lead to warranty claims related to the consuming device when actually it was the consumable which caused the problem. We note that these problems are highlighted in the introductory portion of the specification. Prior solutions have involved using

unique packaging to deter other manufacturers developing generic consumables which could also operate with the consuming device.

The Shigenaga citation is not pertinent to the field of consumables which the applicant's system is designed for. The Shigenaga citation discloses a system used for restricting access to confidential information stored in the IC card using estimated processing time comparisons. Furthermore, the Shigenaga citation is concerned with identifying the card holder of the IC card.

In contrast, the Applicant's system and method relates to determining whether a consumable can be consumed by a consuming device containing authentication chips. The authentication chips allow the system and consuming device to determine whether the consumable is able to be consumed by the consuming device.

The Applicant submits that based on these facts, there is very little to suggest that the Shigenaga citation is pertinent to the field of authenticating consumables. The Shigenaga citation would not logically have commended itself to an inventor's attention in considering his problem relating to authenticating whether a consumable is valid for the particular consuming device, and thus can or cannot be consumed by the consuming device. Thus, the Applicant respectfully submits that the answer to the second question should be answered in the negative by the Examiner.

As the Applicant has respectfully submitted that both questions should be answered in the negative, the Applicant respectfully submits that the Shigenaga should not be considered analogous art. Furthermore, the Applicant respectfully directs the Examiner's attention to the decision in *Wang Laboratories, Inc. v. Toshiba Corp.*, 993 F.2d 858, 26 USPQ2d 1767 (Fed. Cir. 1993). The facts in this case share a striking resemblance to the current case, and as such the Applicant submits that the Examiner should similarly consider the claims as nonobvious in light of Shigenaga in view of Lee.

The Applicant has also included new claims 28 and 29 to specify further distinctions over Shigenaga.

Claim 28 has been introduced to specify that the untrusted chip includes an electronic noise generator to emit electronic noise to restrict detection of processing performed within the untrusted chip. Support for this feature can be found at page 105 under the heading "Noise Generator".

The Applicant submits that Shigenaga fails to disclose an electronic noise generator, and therefore claim 28 is patentable over of Shigenaga in view of Lee.

Claim 29 has also been introduced to specify that the untrusted chip includes a light emitting component operably connected to the electronic noise detector to emit light to restrict detection of processing performed within the untrusted chip. Support for this feature can be found at pages 109 and 110 under the heading "Special implementation of FETs for key data paths" in regard to CMOS inverters and non-Flashing CMOS components.

The Applicant submits that Shigenaga fails to disclose a light emitting component operably connected to the electronic noise detector to restrict detection of processing performed within the untrusted chip, and therefore claim 29 is patentable over Shigenaga in view of Lee.

Reconsideration and withdrawal of this rejection is respectfully requested in light of the above claim amendments and the above comments.

In view of the foregoing, it is respectfully requested that the Examiner reconsider and withdraw the rejections. The present application is believed to be in condition for allowance. Accordingly, the Applicant respectfully requests a Notice of Allowance of all the claims presently under examination.

Very respectfully,
Applicant:

SIMON ROBERT WALMSLEY

C/o: Silverbrook Research Pty Ltd
393 Darling Street
Balmain NSW 2041, Australia

Email: kia.silverbrook@silverbrookresearch.com

Telephone: +612 9818 6633

Facsimile: +61 2 9555 7762